Factors Influencing the Cost of a Risk Assessment

This worksheet provides factors influencing the cost of a risk assessment, and three scenarios incorporating these factors. All scenarios assume the following:

- Maximum 6 week period of performance
- $100 per hour standard rate
- Moderate cooperation from SFA employees and associated contract support
- Travel costs dependent on actual location of facilities and are therefore not included in the cost estimate

The following assessment should be used as a guideline for future risk assessment contract estimations. However, system specific factors will govern the final contract price for each risk assessment. Also, other factors may exist that will influence the final contract price.

Cost Factors:

Time provided to complete Risk Assessment (RA)

Amount/thoroughness of documentation

- Requirements documentation
- Following a lifecycle (SLC)
- Security plan (in 800-18 format)
- Rules of Behavior
- MOU/SLA
- COOP/DRP

Prior assessments/audits/findings

- Available
- Applicable findings highlighted

Interviews/questionnaires

Travel Requirements

System Testing

- Rules of Engagement, lawyers
- Local vs. offsite port scans (Penetration through Vulnerability Scanning)
- Physical vs. Network

Number and location of Facilities

Existence of Reporting Template

Assessor attended Department and SFA Risk Assessment Training

Scenario 1

System A is located in one facility
No travel to the facility will be necessary
No physical or network testing will be performed
A security plan in 800-18 format exists
Prior assessments exist and are in useable format
A formal memorandum of understanding exists describing the interfaces between interconnecting systems
Reporting template exists

Cost estimate: 24K

- # of people: 2
- period of performance: 3 weeks

Scenario 2

System B is located in two facilities in the same geographic location
Travel is required
A vulnerability scan will be performed on one NT Server and one Oracle Database (Need rules of engagement)
A security plan exists in 800-18 format
A requirements document exists
Reporting template exists

Cost estimate + travel: 60K

- # of people: 3
- period of performance: 5 weeks

Scenario 3

System C is located in five facilities around the United States
Travel is required to multiple locations
Vulnerability scanning, penetration testing, physical site examination
Security plan exists, not in 800-18 format
No requirements documentation exists
Very little written security documentation exists
Multiple interviews must be scheduled, conducted, documented, analyzed, incorporated.
Reporting template exists

Cost estimate + travel: 120K +

- # of people: 5
- period of performance: 6 weeks